These are fraudulent schemes to get you to part with your personal details such as passwords/pin numbers and/or cash. Scammers can target you through phishing emails, phone calls, letters, text messages, and in person!

WHAT IS A SCAM?

PHISHING EMAILS

- Attempt to steal your passwords, bank codes and money.
- Provides a link to a website that looks like the real thing.

Common phishing emails can appear to be from:

- Student Finance England (SFE) or Student Loans Company (SLC) - asking you to use a link to add missing details to your account.
- Her Majesty's Revenue and Customs (HMRC) - asking you to use the link provided to get a tax refund.
- UK Visas and Immigration (UKVI) - asking you to use a link to pay money as your visa wasn’t completed properly and you could be removed from the UK.
- Banks - asking you to use a link to confirm your password or pin number.
NEVER USE A LINK TO ACCESS AN OFFICIAL WEBSITE. HYPERLINKS CAN BE SET UP TO TAKE YOU TO ANY WEBSITE!

**TELEPHONE CALLS**

COMMON SCAM CALLS CAN APPEAR TO BE FROM:

- Banks/utility providers saying that there has been fraudulent activity on your account, and asking for your personal details/password/pin number.

Banks will NEVER ask you for these details or ask you for your cards.

- Microsoft telling you there is something wrong with your computer and they can fix it for a fee.

THINGS TO WATCH OUT FOR:

- If they ask you to call your bank etc. to verify their authenticity you can still get conned. If you put your phone down but they don’t disconnect the line – you are talking to them rather than your bank etc. It takes two people to end a phone call!

**BEAT THE SCAMMERS**

- Be suspicious – if it seems too good to be true it probably is.

- Never feel under pressure to agree to anything instantly – take your time and get advice.

- Block suspicious email accounts/phone numbers.

Student Advice and Support Service

www.lboro.ac.uk/services/sass

T. 01509 222058  E. advice@lboro.ac.uk